Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Industrial Security Job Description and Terrorism

FROM: Director of Security
4E-60, Hqs.

EXTENSION

NO.

DATE 31 MAR 1983

STAT
STAT

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. ER 7E-12, Hqs.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

B 312
x F 2054

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Executive Registry
83-1730/2

31 MAR 1983

MEMORANDUM FOR: Executive Assistant to the DDCI

FROM: [redacted] STAT
Director of Security

SUBJECT: Industrial Security Job Description and Terrorism

1. Reference is made to your memorandum of 25 March 1983, which requested a hypothetical job description for an Industrial Security Officer with concerns about terrorism overseas. It was also suggested that we might have some unclassified brochures on terrorism which might be useful to the DDCI in connection with upcoming speeches.

2. Attached herewith as Tab A is an example of an unclassified position description for an Industrial Security Officer employed by a large firm which has offices overseas where there is the terrorist threat. It is emphasized that this is a "hypothetical" job description, drawn upon our own experience in this area. Some of our Security retirees have gotten much more directly involved in the personal protection of business executives in the hostile overseas environment, and their perspective on job requirements might be closer to the mark, should you wish us to pursue this issue.

3. We are not aware of any brochure on terrorism which is distributed through the Department of Commerce. In checking with the Directorate of Intelligence, we were informed that in January, February and March of this year the DDI produced Terrorism Reviews at the Secret level, and I have provided copies for your background information. I have also taken the liberty of attaching a copy of the DDI publications list on the terrorism question, as well as a copy of the Foreign Broadcast Information Service Report, dated 4 February 1983, entitled "Worldwide Report - Terrorism." This report is a thorough and current treatise on international terrorism, but has restricted handling at the "For Official Use Only" level due to copyright laws and government regulations which control ownership and dissemination of the document.

OS 3 0816/A

DCI EXEC REG

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

4. The following unclassified publications might prove to be useful to the DDCI in sessions involving the private sector:

Tab B - Terrorist Attacks Against U. S. Business - June 1982

Tab C - International Terrorism: Hostage Seizures - March 1983

Tab D - Terrorist Skyjackings - July 1982

Tab E - Patterns of International Terrorism: 1981 - July 1982

Tab F - Significant International Terrorist Incidents - (1 April to 30 June 1982)

Tab G - International Terrorism in 1979 - April 1980 (A Research Paper)

Tab H - International Terrorism in 1978 - March 1979 (A Research Paper)

If we can possibly be of any further assistance on this matter, please advise.

STAT

Attachments

Distribution:
Orig - Adse
1 - ER w/o atts B - H
1 - DDA w/o atts B - H

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

POSITION DESCRIPTION: Senior corporate security officer for a large industrial firm which has offices located both within the United States and overseas.

I. GENERAL RESPONSIBILITIES

- Serve as the senior security officer advisor to the President of the company, as well as to all other senior officers, with regard to the physical, technical, personnel and automated data processing security procedures which are to be in effect within the company.

- Be knowledgeable of, and able to conduct appropriate liaison with appropriate security and law enforcement representatives from applicable U.S. Government military and civilian organizations.

- Be knowledgeable of all applicable federal and local statutes and directives which have a bearing on the security of the company's personnel, facilities or operations.

- Prepare and issue guidelines and policies which govern the company's personnel, physical, and technical security procedures.

- Conduct appropriate investigation of prospective employees and/or current employees as required to protect the proprietary interest of the company or with respect to suspected violations of company security policy or violations of law.

- Maintain appropriate liaison with local law enforcement officials who have jurisdiction over U.S. company facilities and offices to ensure that adequate protection of both facilities and personnel is maintained.

- Given the company's overseas business interests, the incumbent must be familiar with local laws and regulations within the host government areas which govern the actions of both company personnel assigned to these locations and/or company representatives visiting these areas. Further, the incumbent must establish liaison with host government law enforcement and security representatives to ensure that adequate protection for company personnel and facilities is maintained, and that any known threats against company resources from any source are made known to appropriate company officers.

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

- Maintain and implement a thorough briefing program for all company personnel relative to personnel protective methods, the protection of proprietary information/ materials, and ensure that the program is in compliance with all appropriate U.S. Government issuances and directives applicable to the company.

- Develop a security organization within the company which will meet the needs of these overall security responsibilities, and participate directly in the recruitment and training of properly qualified personnel to serve within this security organization. Encourage a high degree of specialization within the security disciplines, and maintain an educational program for all members of the security organization to ensure that such employees are kept abreast of new techniques and procedures in the fields of physical, technical, personnel, and automated data processing security.

II. SPECIFIC RESPONSIBILITIES

- Report to the President of the company, and other company officers as appropriate, any information which could have an adverse impact on the personnel, physical or technical security posture of the company.

- Develop and maintain an effective physical security structure which will protect the company's facilities and personnel from hostile threats originating outside the company from a theft, vandalism, and/or terrorist perspective, both domestically and overseas, through the use of guards, physical barriers, locking devices, secure storage containers, and alarms. Arrange for appropriate assistance from either domestic law enforcement agencies or host government security and law enforcement personnel in the event of an incident requiring such assistance.

- Develop an effective emergency plan for use by all employees, customized to meet the needs of each company facility, which can be followed in the event of a national emergency, either domestically or overseas, or in the event of a terrorist attack on company facilities or personnel.

- Develop and maintain an effective personnel security program which will ensure that company personnel meet high standards of character, honesty, integrity, trustworthiness, and loyalty through the utilization of a pre-employment screening procedure which verifies all prospective employees' birth, education, employment record, and reputation among current and former associates.

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

- Ensure that personnel security inquiries are conducted in an appropriate fashion on current employees whenever questions of impropriety and/or violations of law come to your attention. Further, that any allegations of such improprieties or violations of law are promptly reported to appropriate law enforcement agencies and to the President of the company or other appropriate senior company officers.

- Where the company may be involved in contractual relationships with the U.S. Government which involve the receipt and/or fabrication of classified hardware or documents, ensure that all appropriate U.S. Government security issuances, directives, and policies are fully complied with, and that close liaison with security representatives from any such sponsoring U.S. Government entity is maintained.

- Ensure that an in-depth briefing program is maintained for all company personnel to guarantee that all company employees are fully aware of their responsibilities to protect company proprietary interests, classified U.S. Government information where appropriate, and that all company employees are aware of their responsibilities should they be assigned to an overseas location. Cited briefing program should include a complete explanation of the terrorist risks when travelling overseas, and the basic countermeasures which all employees should undertake whenever assigned and/or travelling in foreign countries.

    - This briefing must be tailored for each foreign country where the company has offices, and should provide specific guidance to company employees on basic physical and personnel security practices which they should employ to reduce the threat of their becoming the target of a terrorist attack.

    - Information gleaned from your liaison with appropriate U.S. Government and host foreign security and law enforcement representatives must be used to update such briefngs on a timely basis.

    - A procedure must be developed whereby any specific threats against company personnel or facilities, either domestically or overseas, can be communicated on a timely basis to those concerned.

    - A program must be developed which will allow for a debriefing of all company employees returning from overseas assignment or temporary duty to determine if any unusual incidents occurred. Information gleaned from such debriefings would then be incorporated into the overall briefing program.

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7

- Where applicable for high risk overseas areas, develop and maintain a training program for employees destined for such assignment, either permanently or temporarily, which shall cover the specific techniques employed to avoid becoming the subject of a terrorist attack or kidnap attempt. Such training would include, but not be limited to, defensive driving techniques, personal residence security, methods employed to vary daily habits, and the detection of suspicious contacts with individuals and/or other peculiar incidents which might be indicative of an impending terrorist attack or kidnap attempt.

- Develop and maintain a thorough technical security program which will prevent the compromise of company proprietary information through hostile audio penetrations of company facilities. Ensure that appropriate research and development is conducted in the technical security arena in order that the company may take full advantage of state-of-the-art technological developments in this arena.

- Develop and maintain a thorough security program to prevent hostile intrusion and the resulting compromise of company proprietary information through the company's use of automated data processing systems. Ensure that the company's use of all such automated data processing equipment is handled in a manner consistent with current industrial security procedures to prevent misuse or compromise of such systems. Should classified U.S. Government information be processed on company automated data processing equipment, ensure that all appropriate U.S. Government directives and issuances are followed.

- Implement a security awareness program which will involve periodic rebriefings of all company employees on their security responsibilities, proprietary obligations, and personal conduct requirements, and issue company bulletins and/or posters as appropriate.

- Maintain proper files and other documentation concerning all security facets which deal with the personnel, physical, technical, or automated data processing security matters which will provide an historical data base as well as appropriate records of company procedures and policies in this regard.

- Ensure that company procedures with respect to subcontracting with vendors, suppliers, and/or other sub-contractors contain appropriate stipulations to ensure that any such sub-contractors, vendors, or suppliers protect any company proprietary information which might be made available to them in support of such contractual relationships. In the event classified U.S. Government information is involved, ensure that all applicable U.S. Government directives and issuances relative to such subcontracting are followed.

Approved For Release 2007/12/03 : CIA-RDP85M00364R000701080002-7